This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of securing security data stored on a computer system, comprising ~~the steps of~~:

providing one of several different [a] data keys to the computer system;

transforming the security data with the one data key in a reversible fashion to produce encoded secure data such that the one data key is required in order to perform a reverse transform and extract the security data from the encoded secure data; and,

storing the encoded secure data in a fashion such that a user authorization process is used to retrieve the encoded secure data such that the one data key and the user authorization process, in combination, provide access to the security data and such that the stored data within the computer system is encoded,

wherein a same security data is encoded with said several different data keys to provide several different encoded secure data such that a combination of user authorization and any of said several different data keys allows for retrieval and decoding.

2. Canceled.

3. (Currently Amended) A method of securing security data stored on a computer system according to claim 1, ~~wherein a same security data is encoded with several different data keys to provide several different encoded secure data and~~ wherein each encoded secure data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said several different ~~a plurality of~~ data keys allows for retrieval and decoding.

4. (Original) A method of securing security data stored on a computer system according to claim 1, wherein the user authorization process is a biometric information verification process.

5. (Original) A method of securing security data stored on a computer system according to claim 1, wherein the data keys include a password.

6. (Currently Amended) A method of securing security data stored on a computer system, comprising ~~the steps of~~:

providing a biometric information source and comparing the biometric information source against stored templates associated with the biometric information source[;] and ~~for~~, in dependence upon a comparison result, pairing a biometric information source with a first individual identity;

providing one of several different [a] data keys associated with ~~a second~~ the first individual identity[;], the one data key being other than stored on the computer system; and

retrieving encoded security data associated with the biometric information, and using the ~~key~~ one data key for decoding the encoded security data,

wherein a same security data is encoded with said several different data keys to provide several different encoded secure data such that a combination of user authorization by said biometric information source and any of said several different data keys allows for retrieval and decoding.

7. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for performing at least one of encrypting and decrypting data on the computer system.

8. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for allowing access of the data to the identified individual.

9. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the step of accepting biometric information source comprises imaging the biometric information source using a contact imager.

10. (Original) A method of securing security data stored on a computer system according to claim 9, wherein the contact imager is a fingerprint imager.

11. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing a password.

12. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing information stored on a smart card.

13. (Currently Amended) A method of securing data, comprising ~~the steps of~~:

providing a first information sample to a computer system;

encoding ~~key~~ one of several different data keys in dependence upon the first information sample to produce first security data, the key data for use in decoding stored encoded data;

providing at least one biometric information sample; and

securing the first security data in dependence upon at least one of the at least one biometric information sample,

wherein a same security data is encoded with said several different data keys to provide several different encoded secure data such that a combination of user authorization using said biometric information sample and any of said several different data keys allows for retrieval and decoding.

14. (Currently Amended) A method of securing data as defined in claim 13, wherein the step of providing a first information sample to a computer system comprises ~~the step of:~~ hashing the first information sample to produce a first hash value.

15. (Currently Amended) A method of securing data as defined in claim 13, comprising ~~the steps of~~:

providing a second other information sample to the computer system;

hashing the second information sample to produce a second hash value;

encoding the key data in dependence upon the second hash value to produce second security data; and

securing the second security data in dependence upon at least one of the at least one biometric information sample.

16. (Original) A method of securing data according to claim 13, wherein the step of providing information to a computer system comprises the step of providing a password.

17. (Original) A method of securing data according to claim 13, wherein the step of providing information to a computer system comprises the step of providing information stored on a smart card.

18. (Original) A method of securing data according to claim 13, wherein the key data is used for encrypting data.

19. (Currently Amended) A method of securing data comprising ~~the steps of~~:

providing a first information sample to a computer system;

providing at least one biometric information sample;

encoding the at least one biometric information sample using the first information sample;

encoding ~~key~~ one of several different data keys in dependence upon the encoded biometric sample to produce first security data, the key data for use in decoding stored encoded data; and

securing the first security data in dependence upon at least one of the at least one biometric information sample,

wherein the first security data is encoded with said several different data keys to provide several different encoded secure data such that a combination of user authorization using said biometric information sample and any of said several different data keys allows for retrieval and decoding.

20. (Currently Amended) A method of securing data according to claim 19, comprising ~~comprises the steps of~~:

providing a first information sample to a computer system for decoding the encoded biometric sample; and

comparing the decoded biometric sample against stored templates associated with the biometric information source.

21. (Currently Amended) A method of securing data as defined in claim 19 wherein the step of providing a first information sample to a computer system comprises ~~the step of:~~ hashing the first information sample to produce a first hash value.